

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2002-149475  
(P2002-149475A)

(43)公開日 平成14年5月24日 (2002.5.24)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テマコト <sup>*</sup> (参考)
G 0 6 F 12/00	5 4 6	G 0 6 F 12/00	5 4 6 A 5 B 0 1 7
	5 3 7		5 3 7 A 5 B 0 7 5
12/14	3 2 0	12/14	3 2 0 A 5 B 0 8 2
13/00	5 2 0	13/00	5 2 0 A
17/30	1 1 0	17/30	1 1 0 F

審査請求 未請求 請求項の数 5 O L (全 9 頁) 最終頁に続く

(21)出願番号 特願2000-347471(P2000-347471)

(22)出願日 平成12年11月15日 (2000.11.15)

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番  
1号

(71)出願人 592019877

富士通周辺機株式会社

兵庫県加東郡社町佐保35番

(72)発明者 長谷川 忠

兵庫県加東郡社町佐保35番 富士通周辺機  
株式会社内

(74)代理人 100086933

弁理士 久保 幸雄

最終頁に続く

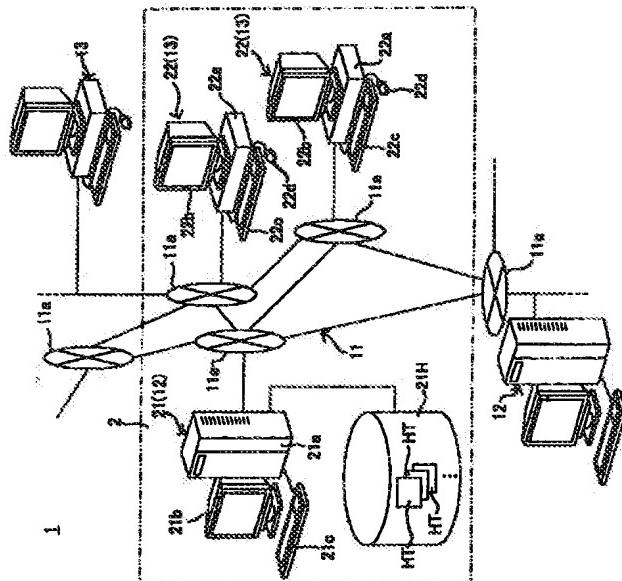
(54)【発明の名称】 ネットワークサーバ、ハイパーテキストの送信制御方法、およびハイパーテキストを記録した記録媒体

インターネットおよびWWWシステムを説明する図

(57)【要約】

【課題】 容易にかつ柔軟に情報資源へのアクセスの制御を行うことができるネットワークサーバ、送信制御方法および記憶媒体を提供する。

【解決手段】 ハイパーテキストHTの送信を制御する送信制御手段を有するWWWサーバ21であって、ハイパーテキストHTは、ハイパーテキストへのアクセスの可否に関する情報であるアクセス可否情報を有し、送信制御手段は、端末装置22からハイパーテキストHTへのアクセスの要求があったときに、アクセス可否情報に基づいて端末装置22へのハイパーテキストHTの送信を制御する。



## 【特許請求の範囲】

【請求項1】ハイパーテキストの送信を制御する送信制御手段を有するネットワークサーバであって、

前記ハイパーテキストは、前記ハイパーテキストへのアクセスの可否に関する情報であるアクセス可否情報を有し、

前記送信制御手段は、クライアントから前記ハイパーテキストへのアクセスの要求があったときに、前記アクセス可否情報に基づいて前記クライアントへの前記ハイパーテキストの送信を制御する、

ことを特徴とするネットワークサーバ。

【請求項2】前記送信制御手段は、前記ハイパーテキストを送信する場合に、前記アクセス可否情報を削除したハイパーテキストを生成して送信する、

請求項1記載のネットワークサーバ。

【請求項3】ハイパーテキストを送信するネットワークサーバと、前記ネットワークサーバへのアクセスが可能なクライアントとからなるネットワークシステムにおいて用いられるハイパーテキストの送信制御方法であつて、

前記ハイパーテキストには、前記ハイパーテキストへのアクセスの可否に関する情報であるアクセス可否情報が記述されており、

前記クライアントから前記ネットワークサーバへ前記ハイパーテキストへのアクセスの要求がなされると、前記ハイパーテキストの前記アクセス可否情報を基に前記クライアントへ前記ハイパーテキストを送信してもよいか否かを判別し、

送信してもよいと判別された場合は、前記ハイパーテキストを送信する、

ことを特徴とするハイパーテキストの送信制御方法。

【請求項4】前記ハイパーテキストを送信する際に、前記アクセス可否情報を削除したハイパーテキストを生成して送信する、

請求項3記載のハイパーテキストの送信制御方法。

【請求項5】ハイパーテキストの送信を制御する送信制御手段を有するコンピュータで読み取り可能な記録媒体であつて、

アクセスの可否に関する情報であるアクセス可否情報が自らの中に記述されたハイパーテキストを記録したコンピュータ読み取り可能な記録媒体。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、HTMLまたはXMLなどの言語で記述されたハイパーテキストを送信するWWWサーバなどのネットワークサーバ、およびハイパーテキストの送信制御方法、並びにハイパーテキストを記録した記録媒体に関する。

## 【0002】

【従来の技術】図10は従来におけるWWWシステム9

を示す図である。従来より、インターネット上に分散した情報資源にアクセスするためのシステムとして、WWWシステムが広く用いられている。

【0003】WWWシステムは、ユーザに提供するための情報資源を管理するWWWサーバ、係るWWWサーバにアクセスするためのWWWブラウザ機能を有するクライアント、通信プロトコルとしてTCP/IPの上位層に位置するHTTP、その他種々の装置またはソフトウェアなどによって実現される。

10 【0004】情報資源は、HTMLまたはXML(Extensible Markup Language)などの言語で記述されるハイパーテキストのファイルとして提供される。ユーザは、クライアントのWWWブラウザにアクセスしたいハイパーテキストのURLを入力して指定する。WWWブラウザは、WWWサーバにそのハイパーテキストへのアクセスを要求し、WWWサーバからそのハイパーテキストをクライアントにダウンロードする。

【0005】例えば、通信プロトコルにHTTPを使用し、サーバ「WWW. xxxx.x.co.jp」上にあるハイパーテキスト「top.html」を指定するURLは、「http://WWW. xxxx.x.co.jp/top.html」となる。

【0006】WWWシステムは、インターネットに限らず、LANまたは幾つかのLANを接続したイントラネットなどにおいても用いられる。さて、大多数のユーザがインターネットを使用している。インターネットは、世界中の大多数のユーザ同士で情報資源を共用することを目的の一つとしており、WWWサーバ上のハイパーテキストへアクセスすることは、原則としてインターネット上のどのクライアントからでも可能である。

【0007】しかし、近年、インターネットの使用方法が多様化し、ハイパーテキストへのアクセスを特定のユーザのみに許可するなど、アクセスを制御したい場合が生じてきた。

【0008】そこで、アクセスを制御する方法が幾つか提案されている。1つは、プロキシサーバなどを用いてファイアウォールを構築する方法である。例えば、ある企業の社内ネットワークとインターネットとの間にファイアウォールを構築し、両者間の通信の制御を行う。ファイアウォールによれば、特定のユーザのみに社内ネットワークからインターネットへのアクセスを許可したり、特定の通信プロトコルによるアクセスの禁止をするなどのアクセス制御を行うことができる。

【0009】もう1つは、ハイパーテキストの置かれている同じディレクトリに図10(b)に示すようなアクセス制御ファイルを設ける方法である。図10(a)に示すWWWシステム9は、インターネット上にあるシステムで、WWWサーバ91およびクライアント92、93などによって実現される。

【0010】WWWサーバ91には、磁気記録装置91

aが設けられており、情報資源であるハイパーテキスト91fが記録されている。磁気記録装置91aの中のハイパーテキスト91fは、ディレクトリ構造によって管理され、1つのディレクトリ91dには、複数個のハイパーテキスト91fおよびそのディレクトリ91dへのアクセスの制御に関する情報が記載されたアクセス制御ファイル91cが記録されている。

【0011】クライアント92、93は、WWWブラウザによってインターネットへのアクセスが可能である。ここで、クライアント92はドメイン「x x x x x. c o. j p」に、クライアント93はドメイン「z z z z z. c o. j p」に属しているとする。

【0012】ユーザは、クライアント92または93のWWWブラウザにハイパーテキスト91fのURLを入力し、ハイパーテキスト91fへのアクセスを要求する。係る要求は、WWWサーバ91へ送信される。

【0013】WWWサーバ91は、ハイパーテキスト91fと同じディレクトリ91dにあるアクセス制御ファイル91cを参照し、ハイパーテキスト91fを要求のあったクライアントへ送信してもよいか否かを判断する。

【0014】図10(b)に記述するアクセス制御ファイル91cは、ドメイン「x x x x x. c o. j p」からのアクセスを許可(a l l o w)し、その他すべてのドメイン(a l l)からのアクセスを拒否(d e n y)する旨の内容である。したがって、この場合、クライアント92からの要求に対してはアクセスを許可し、ハイパーテキスト91fをクライアント92へ送信する。一方、クライアント93からの要求に対してはアクセスを拒否し、その旨のメッセージをクライアント93へ送信する。

【0015】

【発明が解決しようとする課題】しかし、上に述べたファイアウォールによるアクセスの制御は、その管理者でなければアクセスの制御の設定を行うことができず、しかも、その設定に際して高度な知識が必要とされる。設定を誤れば、システム全体のセキュリティを損なう恐れがあるからである。また、ファイルごとにアクセスの制御の設定を行うことができない。したがって、細かなアクセス制御を行うには、ファイアウォールによる方法は適さない。

【0016】一方、アクセス制御ファイル91cを設ける方法は、ディレクトリごとにアクセスの制御が可能であり、多数の者(Webサイトなどを開設し、Webコンテンツなどの情報資源を提供している者)にサービスを提供しているインターネットプロバイダなどにしばしば用いられる。インターネットプロバイダは、各情報提供者にディレクトリを与える。各情報提供者は、自分のディレクトリ内に情報資源であるハイパーテキスト91fを保存し、インターネット上の多数のユーザがハイパ

ーテキスト91fを共用できるようとする。

【0017】1つのディレクトリ91d内に1つのアクセス制御ファイル91cが置かれるので、そのディレクトリ91d内のすべてのハイパーテキスト91fに対して同じアクセス制御がなされる。したがって、ハイパーテキスト91fごとにアクセス制御の設定を行いたい場合は、そのハイパーテキスト91fごとにディレクトリ91dを設けなければならない。

【0018】しかし、本来、ディレクトリとは、ファイルの種類または内容などに応じて管理者にとってファイルの分類を分かり易くするための概念であり、アクセス制御のためにディレクトリを用いると、ファイル管理が煩雑になりがちである。また、WWWサーバ91側でアクセス制御の設定が変更されるたびにハイパーテキスト91fのURLが変更されると、クライアント側のユーザにとってハイパーテキスト91fへのアクセスが不便となる。

【0019】また、アクセス制御ファイル91cは、WWWサーバ91で使用するアクセス制御用のソフトウェアに依存するので、アクセス制御ファイル91cを作成するためには、そのソフトウェアに用いられる言語の文法および規則などを理解しなければならない。さもなければ、誤った記述をしたアクセス制御ファイル91cによって、アクセス制御が正しく行われなかったり、WWWサーバ91全体のセキュリティを損なう恐れが生じることとなる。

【0020】このような理由から、アクセス制御ファイル91cを置くことを禁止するインターネットプロバイダ、またはアクセス制御ファイル91cが存在してもそれを無視するソフトウェアを使用するインターネットプロバイダが多い。

【0021】したがって、上述したいずれの方法によつても、情報資源ごとにアクセスを制御することは困難である。本発明は、このような問題点に鑑み、容易にかつ柔軟に情報資源へのアクセスの制御を行うことができるネットワークサーバ、送信制御方法および記録媒体を提供することを目的とする。

【0022】

【課題を解決するための手段】本発明に係るネットワークサーバは、ハイパーテキストの送信を制御する送信制御手段を有するネットワークサーバであって、前記ハイパーテキストは、前記ハイパーテキストへのアクセスの可否に関する情報であるアクセス可否情報を有し、前記送信制御手段は、クライアントから前記ハイパーテキストへのアクセスの要求があったときに、前記アクセス可否情報に基づいて前記クライアントへの前記ハイパーテキストの送信を制御する。

【0023】好ましくは、前記送信制御手段は、前記ハイパーテキストを送信する場合に、前記アクセス可否情報を削除したハイパーテキストを生成して送信する。本

発明に係るハイパーテキストの送信制御方法は、ハイパーテキストを送信するネットワークサーバと、前記ネットワークサーバへのアクセスが可能なクライアントとかなるネットワークシステムにおいて、前記ハイパーテキストには、前記ハイパーテキストへのアクセスの可否に関する情報であるアクセス可否情報が記述されており、前記クライアントから前記ネットワークサーバへ前記ハイパーテキストへのアクセスの要求がなされると、前記ハイパーテキストの前記アクセス可否情報を基に前記クライアントへ前記ハイパーテキストを送信してもよいか否かを判別し、前記判別の結果、送信してもよいと判断された場合は、前記ハイパーテキストを送信する。

【0024】好ましくは、前記ハイパーテキストを送信する際に、前記アクセス可否情報をから削除したハイパーテキストを生成して送信する。本発明に係るハイパーテキストを記録した記録媒体は、アクセスの可否に関する情報であるアクセス可否情報が自らの中に記述されたハイパーテキストを記録したコンピュータ読み取り可能な記録媒体である。

#### 【0025】

【発明の実施の形態】図1はインターネット1およびWWWシステム2を説明する図、図2はWWWブラウザ22a1の画面HG1を示す図、図3はWWWサーバ21および端末装置22の機能的構成を示すブロック図、図4はハイパーテキストHTの記述の例を示す図、図5はユーザ名およびパスワードを入力するダイアログボックスDABを示す図である。

【0026】図1に示すように、インターネット1は、通信回線11、電子メール、ネットニュース、ファイル転送、またはWWWなどの種々のサービスを提供するネットワークサーバ12、これらのサービスの提供を受けるクライアントである端末装置13、その他種々の装置またはシステムなどによって構成される。

【0027】通信回線11は、複数のLAN11a同士を相互に接続し、または端末装置13を公衆回線を介してLAN11aに接続するなどして構成される。インターネット1の通信プロトコルとしてTCP/IPが用いられ、さらに、WWWシステム2ではHTTPが用いられる。

【0028】WWWシステム2は、インターネット1の一部の構成を用いた情報提供システムである。特に、WWWサーバ21およびWWWブラウザの機能を備えた端末装置22によって実現される。

【0029】WWWサーバ21は、CPU、RAM、通信制御装置、および磁気ディスク装置21Hなどを備えるサーバ装置本体21a、ディスプレイ装置21b、およびキーボード21cなどによって構成され、端末装置22からのアクセスの要求に応じてハイパーテキストHTの送信を行うネットワークサーバ12である。

【0030】ハイパーテキストHTは、Webコンテンツ

ツをWWWブラウザに表示するためのHTMLまたはXMLなどの言語によって記述されるテキストファイルである。情報提供者は、提供したい情報資源をHTMLなどの言語によって記述し、ハイパーテキストHTを作成する。本実施例において、情報提供者は、ハイパーテキストHTに図4に示すようなアクセス制御タグTGを記述し、ハイパーテキストHTへのアクセスの制御をWWWサーバ21に行わせることができる。詳しくは後に説明する。

10 【0031】磁気ディスク装置21Hには、オペレーティングシステムおよびWWWサーバ21の機能を実現するために必要なアプリケーションなどのプログラム、および端末装置22に提供するためのハイパーテキストHTが集合した文書データベースDBTなどが記録されている。これらのプログラムまたはデータは、必要に応じてRAMに読み込まれ、CPUによって演算処理が行われる。

【0032】端末装置22は、CPU、RAM、および通信装置などを備えた端末装置本体22a、ディスプレイ装置22b、キーボード22c、およびマウス22dなどによって構成される。

20 【0033】端末装置本体22aには、WWWブラウザ22a1がインストールされている。WWWブラウザ22a1は、WWWサーバ21に対してハイパーテキストHTへのアクセスを要求し、係るハイパーテキストHTをダウンロードし、または、ハイパーテキストHTに基づいて文字または画像などによってWebコンテンツを図2に示す画面HG1のように視覚的にユーザに表示する。

30 【0034】図2において、端末装置本体22aのユーザは、ディスプレイ装置22bの表示面に表示される画面HG1を見ながら、所望するハイパーテキストHTのURLをテキストボックスBXに入力しましたハイパリンクHLをクリックするなどしてWWWブラウザ22a1を操作し、ハイパーテキストHTへのアクセスを要求する。

【0035】端末装置22として、主にパーソナルコンピュータまたはワークステーションなどが用いられる。その他、WWWブラウザの機能を有する携帯電話、PHS、ゲーム用機械、またはインタラクティブテレビなど種々の装置が用いられる。

【0036】このような構成によって、WWWサーバ21および端末装置22は、図3に示すような機能的構成が実現される。図3に示すように、WWWサーバ21は、受信手段211、ファイル検索手段212、および送信制御手段213の機能を有する。

【0037】受信手段211は、端末装置22からハイパーテキストHTへのアクセスの要求に関する情報などを受信する。ファイル検索手段212は、文書データベースDBTから係る要求に該当するハイパーテキストH

Tを検索する。

【0038】送信制御手段213は、アクセス可否判別部213a、ファイル生成部213b、およびファイル送信部213cなどからなり、端末装置22へのハイパーテキストHTの送信の制御を行う。

【0039】アクセス可否判別部213aは、ハイパーテキストHTに含まれるアクセス制御タグTGに基づいて、ハイパーテキストHTへのアクセスを許可してもよいか否かを判別する。すなわち、端末装置22へハイパーテキストHTを送信してもよいか否かを判別する。詳しくは後に説明する。

【0040】ファイル生成部213bは、ハイパーテキストHTからアクセス制御タグTGを削除し、端末装置22へ送信するためのハイパーテキストHTを生成する。ファイル送信部213cは、ハイパーテキストHTまたはアクセスの拒否のメッセージなどを要求元の端末装置22へ送信する。

【0041】端末装置22の通信制御手段221は、URLに基づいてハイパーテキストHTへのアクセスを要求し、またはハイパーテキストHTを受信するなど、他の装置との間でデータの送受信を行う。

【0042】ここで、アクセス可否判別部213a、ハイパーテキストHTおよびアクセス制御タグTGについて詳しく説明する。図4において、ハイパーテキストHTは、HTMLによって記述され、アクセス制御タグTGを含んでいる。アクセス制御タグTGは、予めHTMLに定義しておく。WWWサーバ21のアクセス可否判別部213aは、アクセス制御タグTG内の引数に従って、そのハイパーテキストHTへのアクセスを許可するか否かを判断する。

【0043】アクセス制御タグ「<meta access deny [ドメイン1], …, [ドメインk]>」は、引数[ドメインk]に指定するドメインに属する装置からのアクセスを拒否することを意味する。したがって、図4(a)に示すアクセス制御タグ「<meta access deny zzzzz.co.jp>」は、ドメイン「zzzzz.co.jp」からのアクセスを拒否することを意味する。

【0044】アクセス制御タグ「<meta access deny [ドメイン1], …, [ドメインk]>」は、引数[ドメインk]に指定するドメインに属する装置からのアクセスを許可することを意味する。

【0045】アクセス制御タグ「<meta access passwd [ユーザ名1], [パスワード1], …, [ユーザ名k], [パスワードk]>」は、引数[ユーザ名k]に指定するユーザが[パスワードk]に指定するパスワードを入力した場合にアクセスを許可することを意味する。したがって、ユーザ名またはパスワードが合致しない場合は、アクセスを拒否する。

【0046】アクセス制御タグ「<meta acce

s s passwd …>」がハイパーテキストHTに含まれているとき、アクセス可否判別部213aは、要求元の端末装置22に対して図5に示すダイアログボックスDABをユーザに表示するように命令する。ユーザは、図5に示すダイアログボックスDABにユーザ名およびパスワードを入力する。したがって、図4(b)に示すアクセス制御タグ「<meta access passwd John, 7s#Q1>」は、ユーザ名「John」およびパスワード「7s#Q1」の入力がなければ、アクセスを拒否することを意味する。

【0047】次に、ハイパーテキストHTへのアクセスに関する処理について、フローチャートを参照して説明する。図6は端末装置22の処理の流れを示すフローチャート、図7はアクセス拒否のメッセージを表示するWWWブラウザ22a1の画面HG2を示す図、図8はWWWサーバ21の処理の流れを示すフローチャートである。

【0048】図6に示すように、端末装置22において、ユーザはWWWブラウザ22a1によって所望するハイパーテキストHTのURLを指定する(#10)。この要求および端末装置22に関する情報が、インターネット1の中のDNSサーバまたは中継サーバなどを経由して、URLに指定されるWWWサーバ21へ送信される(#11)。

【0049】WWWサーバ21からユーザ名およびパスワードの入力の要求があると(#12でYes)、ユーザはダイアログボックスDABよりユーザ名およびパスワードを入力し、WWWサーバ21に返信する(#13)。

【0050】WWWサーバ21からハイパーテキストHTまたはアクセスの拒否のメッセージなどを受信する(#14)。いずれを受信するかは、WWWサーバ21の処理による。

【0051】受信したハイパーテキストHTまたはメッセージをディスプレイ装置22bの表示面に表示する(#15)。所望するハイパーテキストHTが得られた場合は図2に示すような画面HG1が表示される。アクセスを拒否された場合は、図7に示す画面HG2のように、WWWブラウザ22a1は、その旨のメッセージをユーザに表示する。

【0052】図8において、WWWサーバ21は、端末装置22からハイパーテキストHTのアクセスの要求を受信し(#20)、該当するハイパーテキストHTを検索する(#21)。

【0053】ハイパーテキストHTが存在しない場合(#22でNo)、その旨のエラーメッセージを端末装置22へ送信し(#23)、処理を終了する。ハイパーテキストHTが見つかった場合(#22でYes)、ハイパーテキストHTにアクセス制御タグTGが含まれているか否かを判別する(#24)。

【0054】アクセス制御タグTGが含まれていない場合(#24でNo)、直ちにハイパーテキストHTを要求元の端末装置22へ送信し(#28)、処理を終了する。アクセス制御タグTGが含まれている場合(#24でYes)、アクセス制御タグTGに基づいてアクセスの可否を判別する(#25)。例えば、図4(a)に示すハイパーテキストHTの場合は、ドメイン「zzzz.z.co.jp」に属する端末装置22からアクセスの要求は拒否し、それ以外からのアクセスの要求は許可すると判別する。図4(b)に示すハイパーテキストHTの場合は、要求元の端末装置22に対してユーザ名およびパスワードを要求し、これによりアクセスの可否を判別する。

【0055】アクセスを許可する場合(#26でYes)、ハイパーテキストHTからアクセス制御タグTGを削除し(#27)、アクセス制御タグTGを持たないハイパーテキストHTを端末装置22へ送信する(#28)。アクセスを許可しない場合(#26でNo)、アクセスを拒否する旨のメッセージを端末装置22へ送信する(#29)。

【0056】本実施形態によれば、情報資源であるハイパーテキストHTに直接アクセス制御に関するアクセス制御タグTGを記述しているので、ハイパーテキストHTごとに容易にかつ柔軟にアクセスの管理を行うことができる。

【0057】また、アクセス制御タグTGを削除したハイパーテキストHTを端末装置22へ送信しているので、アクセス制御に関する情報の漏洩を防止することができる。

【0058】また、アクセス制御タグTGを「meta」タグによって定義しているので、アクセス制御タグTGを削除せずにハイパーテキストHTを端末装置22へ送信しても、WWWブラウザ22a1は、アクセス制御タグTGを読み飛ばしてWebコンテンツを表示することができる。したがって、アクセス制御タグTGを削除しない場合であっても、アクセス制御タグTGの内容がユーザに簡単に知られてしまうことがない。

【0059】なお、本実施形態において、端末装置22の属するドメインをドメインアドレスによって判別したが、IPアドレスによって判別してもよい。また、端末装置22に用いられるオペレーティングシステムまたはWWWブラウザ22a1の種類によってアクセスを制御するアクセス制御タグTGを定義しておいてもよい。

【0060】アクセス制御タグTGは、タグ「<meta access …>」によって定義したが、その他のタグによって定義してもよい。アクセス制御タグTGは、HTMLまたはXML以外の種々の言語に用いることが可能である。

【0061】図9はアクセス制御タグTGの組み合わせの例を示す図である。アクセス制御タグTGを複数組み

合わせることによって、高度なアクセスの管理を行うことができる。例えば、図9(a)に示す組み合わせの場合、ドメイン「xxxxx.co.jp」からのアクセスは無条件に許可し、ドメイン「zzzzz.co.jp」からのアクセスを拒否し、両ドメイン以外のドメインからのアクセスに対してはユーザ名およびパスワードの入力を要求する。

【0062】また、2つ以上の条件を与えるのであれば、「<meta access 条件1 & … &

10 条件k>」のように、論理積の演算子を表す「&」を予め定義しておけばよい。例えば、図9(b)に示す組み合わせの場合、ドメイン「zzzzz.co.jp」からのアクセスについては、ユーザ名およびパスワードの入力を要求し、ドメイン「xxxxx.co.jp」からのアクセスについては他の条件なしに許可することを意味する。

【0063】本実施形態では、WWWシステム2は、インターネット1に設けられているが、インターネットなどローカルなネットワークに設けることも可能である。

20 本実施形態では、ハイパーテキストHTが磁気ディスク装置21Hに記録された例を示したが、それ以外に、ハイパーテキストHTは、RAMまたはROMなどの半導体メモリ、CD-ROM、フロッピー(登録商標)ディスク、メモリカード、または光磁気ディスクなどの可搬媒体などに記録することができる。記録媒体が可搬媒体である場合には、ハイパーテキストHTは可搬媒体の種類に対応するドライブ装置によって読み出され、磁気ディスク装置などに格納されまたは主メモリ上にローディングされまたは処理される。

30 【0064】その他、WWWシステム2、WWWサーバ21、または端末装置22の全体または各部の構成、処理内容、処理順序、またはアクセス制御タグTGの規則などは、本発明の趣旨に沿って適宜変更することができる。

### 【0065】

【発明の効果】本発明によれば、WWWシステムにおいて、容易にかつ柔軟に情報資源へのアクセスの制御を行うことができる。

### 【図面の簡単な説明】

40 【図1】インターネットおよびWWWシステムを説明する図である。

【図2】WWWブラウザの画面を示す図である。

【図3】WWWサーバおよび端末装置の機能的構成を示すブロック図である。

【図4】ハイパーテキストの記述の例を示す図である。

【図5】ユーザ名およびパスワードを入力するダイアログボックスを示す図である。

【図6】端末装置の処理の流れを示すフローチャートである。

50 【図7】アクセス拒否のメッセージを表示するWWWブ

11

ラウザの画面を示す図である。

【図8】WWWサーバの処理の流れを示すフローチャートである。

【図9】アクセス制御タグの組み合わせの例を示す図である。

【図10】従来におけるWWWシステムを示す図である。

【符号の説明】

\*

12

\* 2 WWWシステム（ネットワークシステム）

2 1 WWWサーバ（ネットワークサーバ）

2 1 3 送信制御手段

2 1 H 磁気ディスク装置（記録媒体）

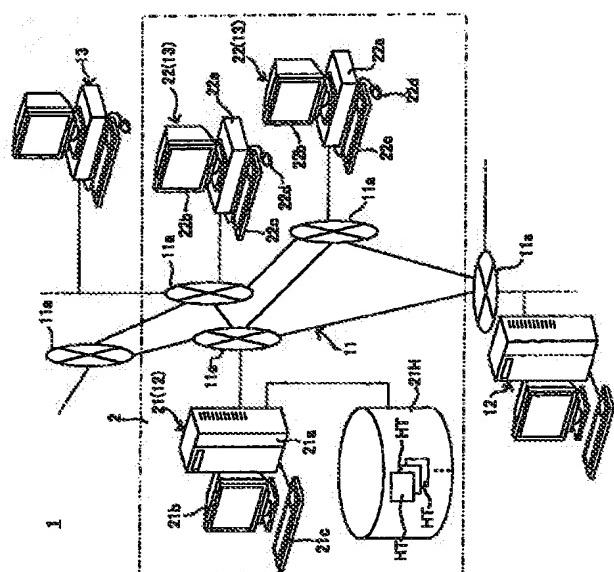
2 2 端末装置（クライアント）

H T ハイパーテキスト

T G アクセス制御タグ（アクセス可否情報）

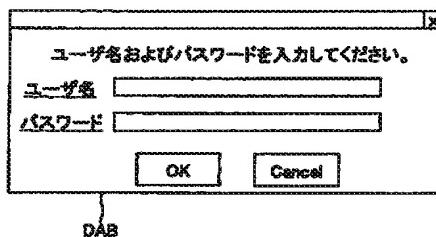
【図1】

インターネットおよびWWWシステムを説明する図



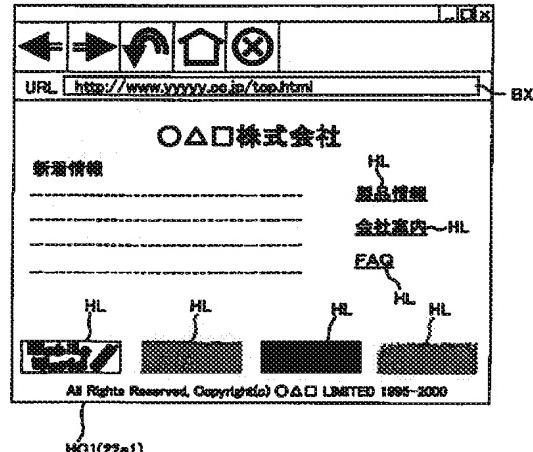
【図5】

ユーザ名およびパスワードを入力するダイアログボックスを示す図



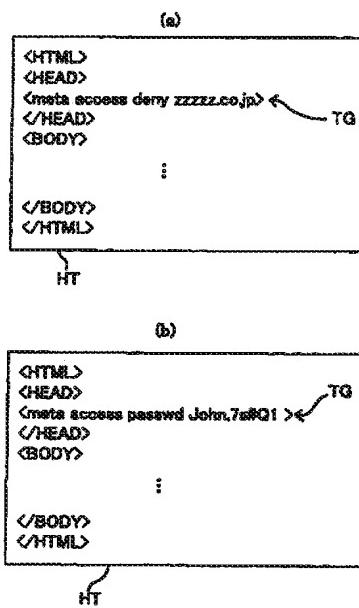
【図2】

WWWブラウザの画面を示す図



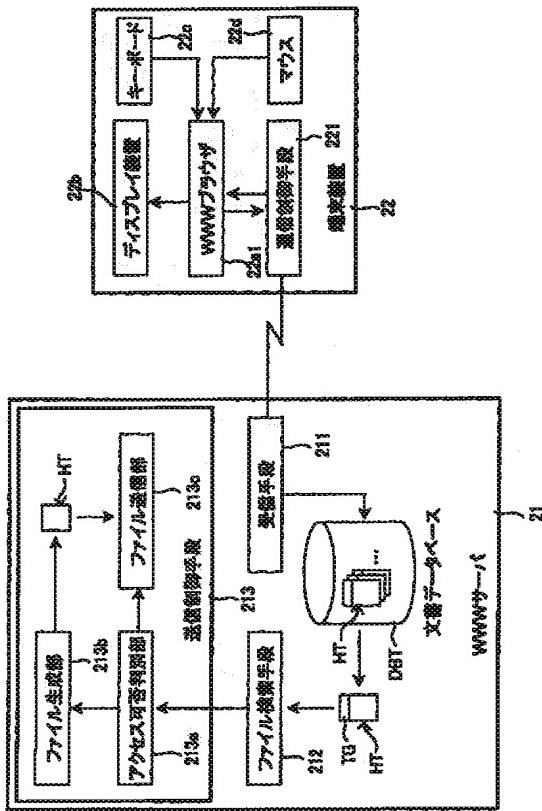
【図4】

ハイパーテキストの記述の例を示す図



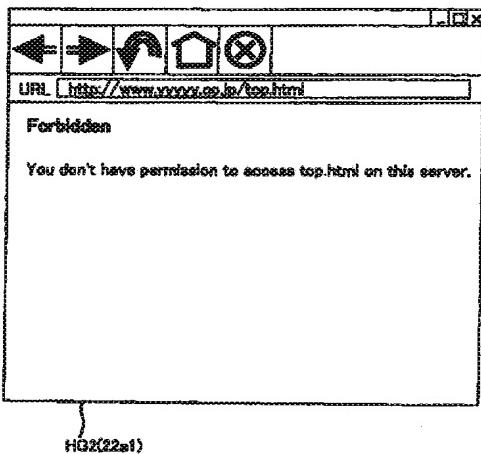
【図3】

WWWサーバおよび端末装置の機能的構成を示すブロック図



【図7】

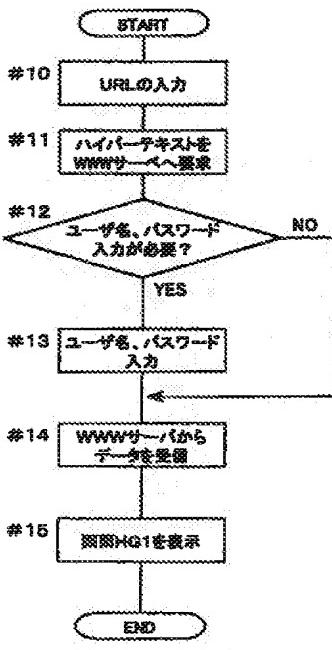
アクセス拒否のメッセージを表示するWWWブラウザの画面の例を示す図



H32(22a1)

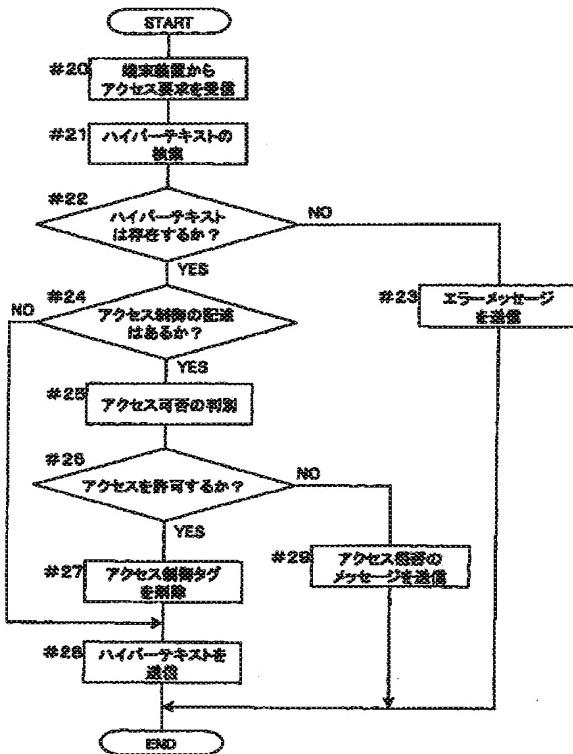
【図6】

端末装置の処理の流れを示すフローチャート



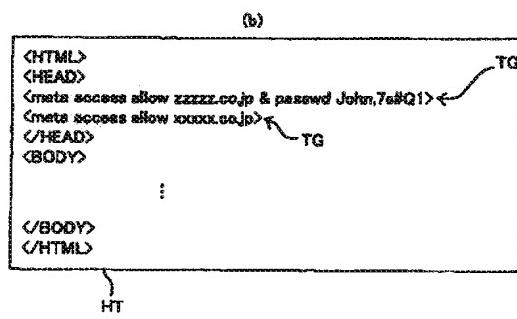
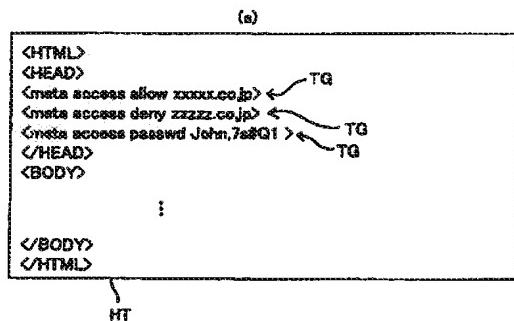
【図8】

WWWサーバの処理の流れを示すフローチャート



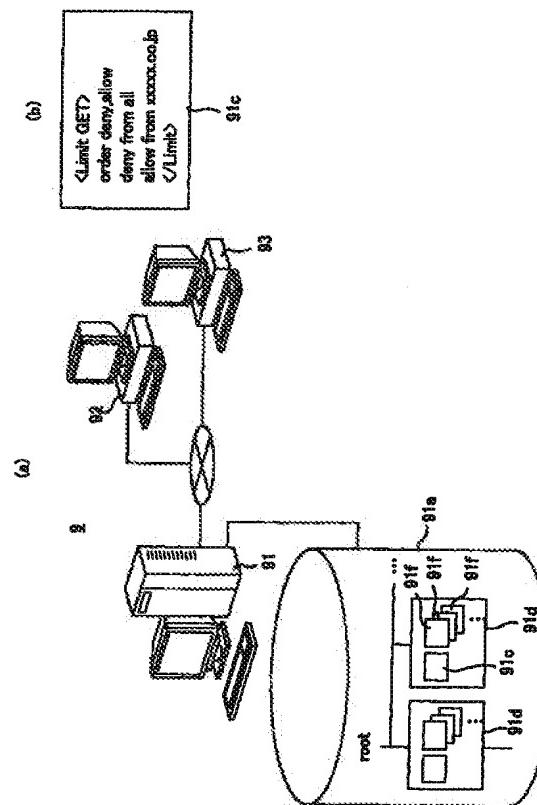
【図9】

アクセス制御タグの応用例を示す図



【図10】

従来におけるWWWシステムを示す図



## フロントページの続き

(51) Int.C1.<sup>7</sup>

G O 6 F 17/30

識別記号

1 2 0

1 7 0

F I

G O 6 F 17/30

「マークド」(参考)

1 2 0 B

1 7 0 A

F ターム(参考) 5B017 AA03 BA06 CA07 CA08 CA09  
CA11 CA12 CA14  
5B075 KK54 ND03 PP03 PQ02 PQ05  
5B082 AA01 BA09 EA11 HA05 HA08